JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Vincent Dupaquis et al. PATENT APPLICATION
Serial No.: 10/781,311 Group Art Unit: 2131
Filed: February 18, 2004
For: RANDOMIZED MODULAR REDUCTION METHOD AND HARDWARE THEREFOR

Supplemental Information Disclosure Statement with Certification under 37 CFR § 1.97(e)(1)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following information is submitted in compliance with Applicants' duty of disclosure under 37 CFR § 1.97(e). A copy of each cited reference is enclosed.

OTHER REFERENCES

Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards, by Jean-François Dhem, Doctorate of Applied Sciences Thesis, Universite Catholique de Louvain, May 1998, pages 11-22.

Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor by Paul Barrett, Security Bulletin, Computer Security Ltd., August 1986.

Efficient Implementation, Handbook of Applied Cryptography, 1997, Menezes, Oorschot, and Vanstone, pages 591-635.

Architectural Tradeoff in Implementing RSA Processors, by Fu-Chi Chang and Chia-Jiu Wang, ACM SIGARCH Computer Architecture News archive, Department of Electrical and Computer Engineering, University of Colorado at Colorado Springs, Colorado, Volume 30, Issue 1, March 2002.

The undersigned hereby certifies that the items of information contained in this Supplemental Information Disclosure Statement were cited in a communication received from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement.

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signed: Brenda Elmidolan
Typed Name: Brenda Elmidolan

Date: April 25, 2005

Respectfully submitted,

David M. Schneck
Reg. No. 43,094

P.O. Box 2-E
San Jose, CA 95109-0005
(408) 297-9733

FORM PTO-1449	Atty. Docket No. ATM-244	Serial No. 10/781,311
LIST OF PRIOR ART CITED BY APPLICANT	Applicants: Vincent Dupaquis et al.	
	Filing Date: February 18, 2004	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						

FOREIGN PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Country	Class	Sub Class	Translation Yes	Translation No
	AK							
	AL							
	AM							
	AN							

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	AO	*Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards* by Jean-Francois Dhem, Doctorate of Applied Sciences Thesis, Universite Catholique de Louvain, May 1998, pages 11-22.
	AP	*Implementing the Rivest Sharmi and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor* by Paul Barrett, Security Bulletin, Computer Security Ltd., August 1986.

EXAMINER:	DATE CONSIDERED:

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449	Atty. Docket No. ATM-244	Serial No. 10/781,311
LIST OF PRIOR ART CITED BY APPLICANT	Applicants: Vincent Dupaquis et al.	
	Filing Date: February 18, 2004	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						

FOREIGN PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Country	Class	Sub Class	Translation Yes No
	AK						
	AL						
	AM						
	AN						

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	AO	*Efficient Implementation*, Handbook of Applied Cryptography, 1997, Menezes, Oorschot, and Vanstone, pages 591-635.
	AP	*Architectural Tradeoff in Implementing RS* Processor by Fu-Chi Chang and Chia-Jiu Wang, ACM SIGARCH Computer Architecture News archive, Department of Electrical and Computer Engineering, University of Colorado at Colorado Springs, Colorado, Volume 30, Issue 1, March 2002.
	AQ	

EXAMINER:	DATE CONSIDERED:

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.